ABSTRACT

A system is described for protecting digital content stored on a storage medium from unauthorized copying. The system includes a number generator to generate a nonce, an encryption subsystem and a decryption subsystem. The encryption subsystem encrypts data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting the encrypted data via a data bus. The encryption bus key is derived based on at least a portion of the key distribution data block, at least one device key assigned to the encryption subsystem and the nonce generated by the number generator. The decryption subsystem is coupled to the data bus to decrypt the encrypted data received over the data bus using a decryption bus key derived based on at least a portion of the key distribution data block, at least one device key assigned to the decryption subsystem and the nonce generated by the number generator.